

NETSPARKER SCAN REPORT SUMMARY

TARGET URL	http://gratia-main-osg.fnal.gov/gratia-admini...	Total Requests	3227
SCAN DATE	5/11/2015 2:58:40 PM	Average Speed	1.15 req/sec.
REPORT DATE	5/12/2015 8:55:25 AM		
SCAN DURATION	00:46:42		

16
identified

5
confirmed

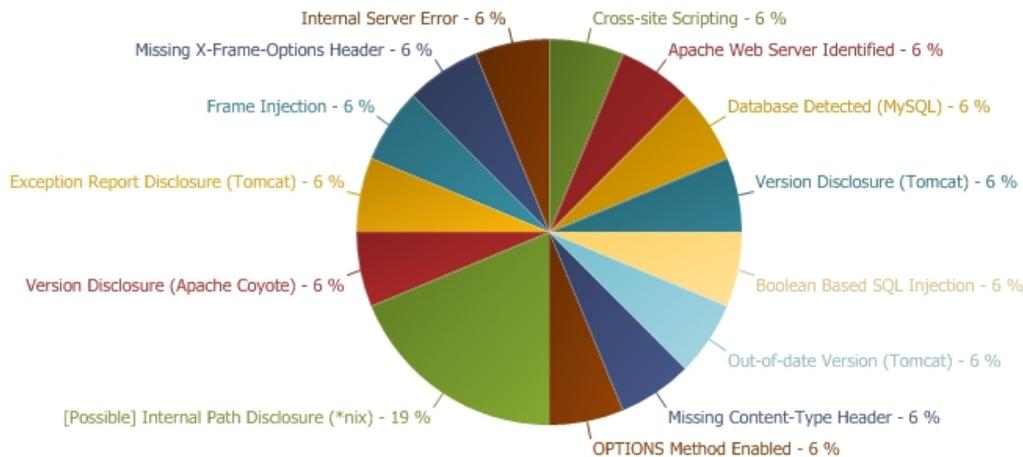
1
critical

6
informational

SCAN SETTINGS

ENABLED ENGINES	SQL Injection, SQL Injection (Boolean), SQL Injection (Blind), Cross-site Scripting, Command Injection, Command Injection (Blind), Local File Inclusion, Remote File Inclusion, Remote Code Evaluation, HTTP Header Injection, Open Redirection, Expression Language Injection, Web App Fingerprint, RoR Code Execution, WebDAV, Reflected File Download, Insecure Reflected Content, XML External Entity, File Upload, Cross-site Scripting (DOM based)	Authentication
		Scheduled

VULNERABILITIES



CRITICAL	6 %
IMPORTANT	6 %
MEDIUM	6 %
LOW	
44	%
INFORMATION	
38	



VULNERABILITY SUMMARY

URL	Parameter	Method	Vulnerability	Confirmed
/gratia-administration/			Version Disclosure (Apache Coyote)	No
			OPTIONS Method Enabled	Yes
			Missing X-Frame-Options Header	No
			Apache Web Server Identified	No
/gratia-administration/adminlogin-howto.jsp			[Possible] Internal Path Disclosure (*nix)	No
/gratia-administration/backlog-byprobes.html			[Possible] Internal Path Disclosure (*nix)	No
/gratia-administration/backlog-history.html	name	GET	Boolean Based SQL Injection	Yes
	name	GET	Cross-site Scripting	Yes
	name	GET	Frame Injection	No
			Database Detected (MySQL)	Yes
/gratia-administration/collector-status.html			Internal Server Error	Yes
/gratia-administration/images/			Version Disclosure (Tomcat)	No
			Out-of-date Version (Tomcat)	No
/gratia-administration/performance-rate.html			Exception Report Disclosure (Tomcat)	No
/gratia-administration/service-configuration-settings.jsp			[Possible] Internal Path Disclosure (*nix)	No
/gratia-administration/site.html			Missing Content-Type Header	No

2. Cross-site Scripting

1 TOTAL

IMPORTANT

CONFIRMED

1

Netsparker detected cross-site scripting, which allows an attacker to execute a dynamic script (*JavaScript*, *VBScript*) in the context of the application.

This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by a user has been interpreted as HTML/JavaScript/VBScript by the browser. Cross-site scripting targets the users of the application instead of the server. Although this is a limitation, since it allows attackers to hijack other users' sessions, an attacker might attack an administrator to gain full control over the application.

Impact

There are many different attacks that can be leveraged through the use of cross-site scripting, including:

- Hijacking user's active session.
- Mounting phishing attacks.
- Intercepting data and performing man-in-the-middle attacks.

Remedy

The issue occurs because the browser interprets the input as active HTML, JavaScript or VBScript. To avoid this, output should be encoded according to the output location and context. For example, if the output goes in to a JavaScript block within the HTML document, then output needs to be encoded accordingly. Encoding can get very complex, therefore it's strongly recommended to use an encoding library such as [OWASP ESAPI](#) and [Microsoft Anti-cross-site scripting](#).

Remedy References

- [Microsoft Anti-XSS Library](#)
- [OWASP XSS Prevention Cheat Sheet](#)
- [OWASP AntiSamy Java](#)

External References

- [XSS Cheat Sheet](#)
- [OWASP - cross-site scripting](#)
- [XSS Shell](#)
- [XSS Tunnelling](#)

Proof of Concept Notes

Generated XSS exploit might not work due to browser XSS filtering. Please follow the guidelines below in order to disable XSS filtering for different browsers. Also note that;

- XSS filtering is a feature that's enabled by default in some of the modern browsers. It should only be disabled temporarily to test exploits and should be reverted back if the browser is actively used other than testing purposes.
- Even though browsers have certain checks to prevent Cross-site scripting attacks in practice there are a variety of ways to bypass this mechanism therefore a web application should not rely on this kind of client-side browser checks.

Chrome

- Open command prompt.
- Go to folder where chrome.exe is located.
- Run the command `chrome.exe --args --disable-xss-auditor`

Internet Explorer

- Click Tools->Internet Options and then navigate to the Security Tab.
- Click Custom level and scroll towards the bottom where you will find that Enable XSS filter is currently Enabled.
- Set it to disabled. Click OK.
- Click Yes to accept the warning followed by Apply.

Firefox

- Go to `about:config` in the URL address bar.
- In the search field, type `urlbar.filter` and find `browser.urlbar.filter.javascript`.
- Set its value to `false` by double clicking the row.

Classification

[OWASP 2010-A2](#) [OWASP 2013-A3](#) [PCI V2.0-6.5.7](#) [PCI V3.0-6.5.7](#) [PCI V3.1-6.5.7](#) [CWE-79](#) [CAPEC-19](#) [WASC-08](#)

4. Internal Server Error

1 TOTAL

LOW

CONFIRMED

1

Netsparker identified an internal server error.

The server responded with an HTTP status 500, indicating there is a server-side error. Reasons may vary, and the behavior should be analyzed carefully. If Netsparker is able to find a security issue in the same resource, it will report this as a separate vulnerability.

Impact

The impact may vary depending on the condition. Generally this indicates poor coding practices, not enough error checking, sanitization and whitelisting. However, there might be a bigger issue, such as SQL injection. If that's the case, Netsparker will check for other possible issues and report them separately.

Remedy

Analyze this issue and review the application code in order to handle unexpected errors; this should be a generic practice, which does not disclose further information upon an error. All errors should be handled server-side only.

4.1. /gratia-administration/collector-status.html **CONFIRMED**

<http://gratia-main-osg.fnal.gov/gratia-administration/collector-status.html?hTTP://r87.com/n>

Parameters

Parameter	Type	Value
out	GET	html
Query Based	Query String	hTTP://r87.com/n

Request

```
GET /gratia-administration/collector-status.html?hTTP://r87.com/n HTTP/1.1
Cache-Control: no-cache
Referer: http://gratia-main-osg.fnal.gov/gratia-administration/dashboard.jsp
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: gratia-main-osg.fnal.gov
Cookie: JSESSIONID=F1ED407F3CE0DDCFA012559C1794128E
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 500 Internal Server Error
Connection: close
Date: Mon, 11 May 2015 19:59:42 GMT
Server: Apache-Coyote/1.1
Content-Length: 1372
Content-Type: text/html;charset=utf-8

<html><head><title>Apache Tomcat/6.0.24 - Error report</title><style><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P {font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color : #525D76;}--></style> </head><body><h1>HTTP Status 500 - </h1><hr size="1" noshade="noshade"><p><b>type</b> Exception report</p><p><b>message</b> <u></u><p><b>description</b> <u>The server encountered an internal error () that prevented it from fulfilling this request.</u></p><p><b>exception</b> <pre>java.lang.NullPointerException
net.sf.gratia.administration.CollectorStatus.doGet(Unknown Source)
javax.servlet.http.HttpServlet.service(HttpServlet.java:617)
javax.servlet.http.HttpServlet.service(HttpServlet.java:717)
</pre></p><p><b>note</b> <u>The full stack trace of the root cause is available in the Apache Tomcat/6.0.24 logs.</u></p><hr size="1" noshade="noshade"><h3>Apache Tomcat/6.0.24</h3></body></html>
```

5. Version Disclosure (Tomcat)

1 TOTAL

LOW

Netsparker identified a version disclosure (Tomcat) in target web server's HTTP response.

This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of Tomcat.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Remedy

Configure your web server to prevent information leakage from the `X-Powered-By` header of its HTTP response.

Remedy References

- [OWASP Securing Tomcat](#)

Classification

[CWE-205](#) [CAPEC-170](#) [WASC-45](#)

5.1. /gratia-administration/images/

<http://gratia-main-osg.fnal.gov/gratia-administration/images/>

Extracted Version

6.0.24

Certainty



Request

```
GET /gratia-administration/images/ HTTP/1.1
Cache-Control: no-cache
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: gratia-main-osg.fnal.gov
Cookie: JSESSIONID=F1ED407F3CE0DDCFA012559C1794128E
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 404 Not Found
Date: Mon, 11 May 2015 19:58:47 GMT
Server: Apache-Coyote/1.1
Content-Length: 1042
Content-Type: text/html;charset=utf-8

<html><head><title>Apache Tomcat/6.0.24 - Error report</title><style><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-
size:14px;} BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color : #525D76;}--></style> </head><body>
<h1>HTTP Status 404 - /gratia-administration/images/</h1><hr size="1" noshade="noshade"><p><b>type</b><b> Status report</p><p><b>message</b></p></u></gratia-
administration/images/</u><p><b>description</b></p><u>The requested resource (/gratia-administration/images/) is not available.</u></p><hr size="1" noshade="noshade">
<h3>Apache Tomcat/6.0.24</h3></body></html>
```

6. Version Disclosure (Apache Coyote)

1 TOTAL

LOW

Netsparker identified a version disclosure (Apache Coyote) in target web server's HTTP response.

This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of Apache.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Remedy

Configure your web server to prevent information leakage from the `SERVER` header of its HTTP response.

Classification

[CWE-205](#) [CAPEC-170](#) [WASC-45](#)

6.1. /gratia-administration/

<http://gratia-main-osg.fnal.gov/gratia-administration/>

Extracted Version

Apache-Coyote/1.1

Certainty



Request

```
GET /gratia-administration/ HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: gratia-main-osg.fnal.gov
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Date: Mon, 11 May 2015 19:58:40 GMT
Server: Apache-Coyote/1.1

Accept-Ranges: bytes
ETag: W/"1038-1409755330000"
Content-Length: 1038
Content-Type: text/html
Last-Modified: Wed, 03 Sep 2014 14:42:10 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Frameset//EN" "http://www.w3.org/TR/html4/frameset.dtd">

<html>
<head>
<meta http-equiv="expires" content="-1">
<meta http-equiv="pragma" content="no-cache">
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
<meta http-equiv="Content-Language" content="en-GB">
<script language="javascript1.2" type="text/javascript">
<!--
// This page avoit to be shown under frames
if (top.frames.length!=0) top.location=self.document.location;
//-->
</script>

<link href="stylesheet.css" type="text/css" rel="stylesheet">
<title>Gratia Accounting - Administration</title>
</head>
<frameset cols="21%,*">
<frame src="./dashboard.jsp" name="adminDashboard" id="adminDashboard" scrolling="auto" frameborder="1">
<frameset rows="37,*">
<frame src="admininfo.jsp" name="adminInfo" id="adminInfo" scrolling="no" frameborder="0">
<frame src="" name="adminContent" id="adminContent" scrolling="auto" frameborder="0">
</frameset>
</frameset>
</html>
```

7. Exception Report Disclosure (Tomcat)

1 TOTAL

LOW

Netsparker identified an exception report disclosure (Tomcat) in the target web server's HTTP response.

Impact

An attacker can obtain information such as:

- Tomcat version.
- Physical file path of Tomcat files.
- Information about the generated exception.

This information might help an attacker gain more information and potentially focus on the development of further attacks to the target system.

Remedy

Apply the following configuration to your `web.xml` file to prevent information leakage by applying custom error pages.

```
<error-page>
  <error-code>500</error-code>
  <location>/server_error.html</location>
</error-page>
```

Remedy References

- [Custom Error Pages on Tomcat](#)

Classification

[OWASP 2010-A6](#) [OWASP 2013-A5](#) [PCI V2.0-6.5.5](#) [PCI V3.0-6.5.5](#) [PCI V3.1-6.5.5](#) [CWE-600](#) [CAPEC-214](#) [WASC-14](#)

7.1. /gratia-administration/performance-rate.html

<http://gratia-main-osg.fnal.gov/gratia-administration/performance-rate.html?housekeepingDetails=yes>

Certainty



Request

```
GET /gratia-administration/performance-rate.html?housekeepingDetails=yes HTTP/1.1
Cache-Control: no-cache
Referer: http://gratia-main-osg.fnal.gov/gratia-administration/performance-rate.html
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: gratia-main-osg.fnal.gov
Cookie: JSESSIONID=F1ED407F3CE0DDCFA012559C1794128E
Accept-Encoding: gzip, deflate
```

Response

```
...
noshade"><p><b>type</b> Exception report</p><p><b>message</b> <u></u><p><b>description</b> <u>The server encountered an internal error () that prevented it from fulfilling this request.</u></p><b>exception</b> <pre>javax.servlet.ServletException: Servlet execution threw an exception
</pre><p><b>root cause</b> <pre>java.lang.OutOfMemoryError: Java heap space
java.util.Arrays.copyOf(Arrays.java:2219)
java.util.ArrayList.grow(ArrayList.java:242)
java.util.ArrayList.ensureExplicitCapacity(ArrayList.java:216)
java.util.ArrayList.ensureCapacityInternal(ArrayList.java:208)
java.util.ArrayList.add(ArrayList.java:440)
com.mysql.jdbc.MysqlIO.readSingleRowSet(MysqlIO.java:3554)
com.mysql.jdbc.MysqlIO.getResultSet(MysqlIO.java:489)
com.mysql.jdbc.MysqlIO.readResultsForQueryOrUpdate(MysqlIO.java:3240)
com.mysql.jdbc.MysqlIO.readAllResults(MysqlIO.java:2411)
com.mysql.jdbc.MysqlIO.sqlQueryDirect(MysqlIO.java:2834)
com.mysql.jdbc.ConnectionImpl.execSQL(ConnectionImpl.java:2838)
com.mysql.jdbc.PreparedStatement.executeInternal(PreparedStatement.java:2082)
com.mysql.jdbc.PreparedStatement.executeQuery(PreparedStatement.java:2212)
net.sf.gratia.administration.PerformanceRates.GetRecordNumberXml(Unknown Source)
net.sf.gratia.administration.PerformanceRates.appendHouseKeeping(Unknown Source)
net.sf.gratia.administration.PerformanceRates.process(Unknown Source)
net.sf.gratia.administration.PerformanceRates.doGet(Unknown Source)
javax.servlet.http.HttpServlet.service(HttpServlet.java:617)
javax.servlet.http.HttpServlet.service(HttpServlet.java:717)
</pre><p><b>note</b> <u>The full stack trace of the root cause is available in the Apache Tomcat/6.0.24 logs.</u></p><hr size="1" noshade="noshade"></h3>A
...

```

8. OPTIONS Method Enabled

1 TOTAL

LOW

CONFIRMED

1

Netsparker detected that `OPTIONS` method is allowed. This issue is reported as extra information.

Impact

Information disclosed from this page can be used to gain additional information about the target system.

Remedy

Disable `OPTIONS` method in all production systems.

External References

- [Testing for HTTP Methods and XST \(OWASP-CM-008\)](#)
- [HTTP/1.1: Method Definitions](#)

Classification

[OWASP 2010-A6](#) [OWASP 2013-A5](#) [CWE-16](#) [CAPEC-107](#) [WASC-14](#)

8.1. /gratia-administration/ **CONFIRMED**

<http://gratia-main-osg.fnal.gov/gratia-administration/>

Allowed methods

GET, HEAD, POST, PUT, DELETE, OPTIONS

Request

```
OPTIONS /gratia-administration/ HTTP/1.1
Cache-Control: no-cache
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: gratia-main-osg.fnal.gov
Cookie: JSESSIONID=F1ED407F3CE0DDCFA012559C1794128E
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Date: Mon, 11 May 2015 19:58:49 GMT
Server: Apache-Coyote/1.1
Allow: GET, HEAD, POST, PUT, DELETE, OPTIONS
Content-Length: 0
```

9. Missing X-Frame-Options Header

1 TOTAL

LOW

Netsparker detected a missing `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.

The `X-Frame-Options` HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a `frame` or an `iframe`. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

Impact

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Remedy

- Sending the proper `X-Frame-Options` in HTTP response headers that instruct the browser to not allow framing from other domains.
- Employing defensive code in the UI to ensure that the current frame is the most top level window.

Remedy References

- [Clickjacking Defense Cheat Sheet](#)

External References

- [Clickjacking](#)

Classification

[OWASP 2010-A6](#) [OWASP 2013-A5](#) [CWE-693](#) [CAPEC-103](#)

9.1. /gratia-administration/

<http://gratia-main-osg.fnal.gov/gratia-administration/>

Certainty



Request

```
GET /gratia-administration/ HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: gratia-main-osg.fnal.gov
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Date: Mon, 11 May 2015 19:58:40 GMT
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"1038-1409755330000"
Content-Length: 1038
Content-Type: text/html
Last-Modified: Wed, 03 Sep 2014 14:42:10 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Frameset//EN" "http://www.w3.org/TR/html4/frameset.dtd">

<html>
<head>
<meta http-equiv="expires" content="-1">
<meta http-equiv="pragma" content="no-cache">
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
<meta http-equiv="Content-Language" content="en-GB">
<script language="javascript1.2" type="text/javascript">
<!--
// This page avoid to be shown under frames
if (top.frames.length!=0) top.location=self.document.location;
//-->
</script>

<link href="stylesheet.css" type="text/css" rel="stylesheet">
<title>Gratia Accounting - Administration</title>
</head>
<frameset cols="21%,*">
<frame src="/dashboard.jsp" name="adminDashboard" id="adminDashboard" scrolling="auto" frameborder="1">
<frameset rows="37,*">
<frame src="admininfo.jsp" name="adminInfo" id="adminInfo" scrolling="no" frameborder="0">
<frame src="" name="adminContent" id="adminContent" scrolling="auto" frameborder="0">
</frameset>
</frameset>
</html>
```

10. Missing Content-Type Header

1 TOTAL

LOW

Netsparker detected a missing `Content-Type` header which means that this website could be at risk of a MIME-sniffing attacks.

Impact

MIME type sniffing is a standard functionality in browsers to find an appropriate way to render data where the HTTP headers sent by the server are either inconclusive or missing.

This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the intended content type.

The problem arises once a website allows users to upload content which is then published on the web server. If an attacker can carry out XSS (Cross-site Scripting) attack by manipulating the content in a way to be accepted by the web application and rendered as HTML by the browser, it is possible to inject code in e.g. an image file and make the victim execute it by viewing the image.

Remedy

1. When serving resources, make sure you send the content-type header to appropriately match the type of the resource being served. For example, if you are serving an HTML page, you should send the HTTP header:

```
Content-Type: text/html
```

2. Add the X-Content-Type-Options header with a value of "nosniff" to inform the browser to trust what the site has sent is the appropriate content-type, and to not attempt "sniffing" the real content-type.

```
X-Content-Type-Options: nosniff
```

External References

- [MIME Sniffing: feature or vulnerability?](#)

Classification

[OWASP 2010-A6](#) [OWASP 2013-A5](#)

10.1. /gratia-administration/site.html

<http://gratia-main-osg.fnl.gov/gratia-administration/site.html>

Certainty



Request

```
GET /gratia-administration/site.html HTTP/1.1
Cache-Control: no-cache
Referer: http://gratia-main-osg.fnl.gov/gratia-administration/dashboard.jsp
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: gratia-main-osg.fnl.gov
Cookie: JSESSIONID=F1ED407F3CE0DDCFA012559C1794128E
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 302 Moved Temporarily
Date: Mon, 11 May 2015 19:58:47 GMT
Server: Apache-Coyote/1.1
Location: https://gratia-main-osg.fnl.gov:443/gratia-administration/gratia-login.jsp
Content-Length: 0
```


12. Out-of-date Version (Tomcat)

1 TOTAL
INFORMATION

Netsparker identified you are using an out-of-date version of Tomcat.

Remedy

Please upgrade your installation of Tomcat to the latest stable version.

Remedy References

- [Apache Tomcat Versions and Download](#)

Known Vulnerabilities in this Version

Apache Tomcat SecurityManager Security Bypass Vulnerability

Apache Tomcat, when running within a SecurityManager, does not make the ServletContext attribute read-only, which allows local web applications to read or write files outside of the intended working directory, as demonstrated using a directory traversal attack.

External References

- [CVE-2010-3718](#)

Apache Tomcat 'Transfer-Encoding' Information Disclosure and Denial Of Service Vulnerabilities

Apache Tomcat does not properly handle an invalid Transfer-Encoding header, which allows remote attackers to cause a denial of service (application outage) or obtain sensitive information via a crafted header that interferes with "recycling of a buffer."

External References

- [CVE-2010-2227](#)

Exploit

- http://www.metasploit.com/modules/auxiliary/dos/http/apache_tomcat_transfer_encoding

Apache Tomcat Authentication Header Realm Name Information Disclosure Vulnerability

Apache Tomcat might allow remote attackers to discover the server's hostname or IP address by sending a request for a resource that requires BASIC or DIGEST authentication, and then reading the realm field in the WWW-Authenticate header in the reply.

External References

- [CVE-2010-1157](#)

Exploit

- <http://www.exploit-db.com/exploits/12343/>

Apache Tomcat HTML Manager Interface HTML Injection Vulnerability

Multiple cross-site scripting (XSS) vulnerabilities in the HTML Manager Interface in Apache Tomcat allow remote attackers to inject arbitrary web script or HTML, as demonstrated via the display-name tag.

External References

- [CVE-2011-0013](#)

Apache Tomcat NIO Connector Denial of Service Vulnerability

Apache Tomcat does not enforce the maxHttpHeaderSize limit for requests involving the NIO HTTP connector, which allows remote attackers to cause a denial of service (OutOfMemoryError) via a crafted request.

External References

- [CVE-2011-0534](#)

Apache Tomcat HTTP DIGEST Authentication Multiple Security Weaknesses

The HTTP Digest Access Authentication implementation in Apache Tomcat does not have the expected countermeasures against replay attacks, which makes it easier for remote attackers to bypass intended access restrictions by sniffing the network for valid requests, related to lack of checking of nonce (aka server nonce) and nc (aka nonce-count or client nonce count) values.

External References

- [CVE-2011-1184](#)

Apache Tomcat 'MemoryUserDatabase' Information Disclosure Vulnerability

Apache Tomcat, when the MemoryUserDatabase is used, creates log entries containing passwords upon encountering errors in JMX user creation, which allows local users to obtain sensitive information by reading a log file.

External References

- [CVE-2011-2204](#)

Apache Tomcat 'sendfile' Request Attributes Information Disclosure Vulnerability

Apache Tomcat, when sendfile is enabled for the HTTP APR or HTTP NIO connector, does not validate certain request attributes, which allows local users to bypass intended file access restrictions or cause a denial of service (infinite loop or JVM crash) by leveraging an untrusted web application.

External References

- [CVE-2011-2526](#)

Apache Tomcat AJP Protocol Security Bypass Vulnerability

Certain AJP protocol connector implementations in Apache Tomcat, and possibly other versions allow remote attackers to spoof AJP requests, bypass authentication, and obtain sensitive information by causing the connector to interpret a request body as a new request.

External References

- [CVE-2011-3190](#)

Apache Tomcat Parameter Handling Denial of Service Vulnerability

Apache Tomcat 5.5.x before 5.5.35, 6.x before 6.0.34, and 7.x before 7.0.23 uses an inefficient approach for handling parameters, which allows remote attackers to cause a denial of service (CPU consumption) via a request that contains many parameters and parameter values, a different vulnerability than CVE-2011-4858.

External References

- [CVE-2012-0022](#)

Apache Tomcat HTTP DIGEST Authentication Multiple Security Weaknesses

DigestAuthenticator.java in the HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.34, 6.x before 6.0.33, and 7.x before 7.0.12 uses Catalina as the hard-coded server secret (aka private key), which makes it easier for remote attackers to bypass cryptographic protection mechanisms by leveraging knowledge of this string, a different vulnerability than CVE-2011-1184.

External References

- [CVE-2011-5064](#)

Apache Tomcat and the hashtable collision DoS vulnerability

Apache Tomcat before 5.5.35, 6.x before 6.0.35, and 7.x before 7.0.23 computes hash values for form parameters without restricting the ability to trigger hash collisions predictably, which allows remote attackers to cause a denial of service (CPU consumption) by sending many crafted parameters.

External References

- [CVE-2011-4858](#)

Apache Commons Daemon 'jsvc' Information Disclosure Vulnerability

native/unix/native/jsvc-unix.c in jsvc in the Daemon component 1.0.3 through 1.0.6 in Apache Commons, as used in Apache Tomcat 5.5.32 through 5.5.33, 6.0.30 through 6.0.32, and 7.0.x before 7.0.20 on Linux, does not drop capabilities, which allows remote attackers to bypass read permissions for files via a request to an application.

External References

- [CVE-2011-2729](#)

Apache Tomcat CVE-2012-2733 Denial of Service Vulnerability

java/org/apache/coyote/http11/InternalNioInputBuffer.java in the HTTP NIO connector in Apache Tomcat 6.x before 6.0.36 and 7.x before 7.0.28 does not properly restrict the request-header size, which allows remote attackers to cause a denial of service (memory consumption) via a large amount of header data.

External References

- [CVE-2012-2733](#)

Apache Tomcat CVE-2012-5568 Denial of Service Vulnerability

Apache Tomcat through 7.0.x allows remote attackers to cause a denial of service (daemon outage) via partial HTTP requests, as demonstrated by Slowloris.

External References

- [CVE-2012-5568](#)

Apache Tomcat DIGEST Authentication Multiple Security Weaknesses

The replay-countermeasure functionality in the HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.36, 6.x before 6.0.36, and 7.x before 7.0.30 tracks cnonce (aka client nonce) values instead of nonce (aka server nonce) and nc (aka nonce-count) values, which makes it easier for remote attackers to bypass intended access restrictions by sniffing the network for valid requests, a different vulnerability than CVE-2011-1184.

External References

- [CVE-2012-5885](#)

Apache Tomcat DIGEST Authentication Multiple Security Weaknesses

The HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.36, 6.x before 6.0.36, and 7.x before 7.0.30 caches information about the authenticated user within the session state, which makes it easier for remote attackers to bypass authentication via vectors related to the session ID.

External References

- [CVE-2012-5886](#)

Apache Tomcat DIGEST Authentication Multiple Security Weaknesses

The HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.36, 6.x before 6.0.36, and 7.x before 7.0.30 does not properly check for stale nonce values in conjunction with enforcement of proper credentials, which makes it easier for remote attackers to bypass intended access restrictions by sniffing the network for valid requests.

External References

- [CVE-2012-5887](#)

Apache Tomcat Session Fixation Vulnerability

java/org/apache/catalina/authenticator/FormAuthenticator.java in the form authentication feature in Apache Tomcat 6.0.21 through 6.0.36 and 7.x before 7.0.33 does not properly handle the relationships between authentication requirements and sessions, which allows remote attackers to inject a request into a session by sending this request during completion of the login form, a variant of a session fixation attack.

External References

- [CVE-2013-2067](#)

📄 Apache Tomcat Denial of Service Vulnerability

Integer overflow in the parseChunkHeader function in java/org/apache/coyote/http11/filters/ChunkedInputFilter.java in Apache Tomcat before 6.0.40, 7.x before 7.0.53, and 8.x before 8.0.4 allows remote attackers to cause a denial of service (resource consumption) via a malformed chunk size in chunked transfer coding of a request during the streaming of data.

External References

- [CVE-2014-0075](#)

📄 Apache Tomcat Restriction Bypass Vulnerability

java/org/apache/catalina/servlets/DefaultServlet.java in the default servlet in Apache Tomcat before 6.0.40, 7.x before 7.0.53, and 8.x before 8.0.4 does not properly restrict XSLT stylesheets, which allows remote attackers to bypass security-manager restrictions and read arbitrary files via a crafted web application that provides an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue.

External References

- [CVE-2014-0096](#)

📄 Apache Tomcat Integer Overflow Vulnerability

Integer overflow in java/org/apache/tomcat/util/buf/Ascii.java in Apache Tomcat before 6.0.40, 7.x before 7.0.53, and 8.x before 8.0.4, when operated behind a reverse proxy, allows remote attackers to conduct HTTP request smuggling attacks via a crafted Content-Length HTTP header.

External References

- [CVE-2014-0099](#)

📄 Apache Tomcat XXE Vulnerability

Apache Tomcat before 6.0.40, 7.x before 7.0.54, and 8.x before 8.0.6 does not properly constrain the class loader that accesses the XML parser used with an XSLT stylesheet, which allows remote attackers to (1) read arbitrary files via a crafted web application that provides an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue, or (2) read files associated with different web applications on a single Tomcat instance via a crafted web application.

External References

- [CVE-2014-0119](#)

📄 Apache Tomcat Denial of Service Vulnerability

java/org/apache/coyote/http11/filters/ChunkedInputFilter.java in Apache Tomcat 6.x before 6.0.42, 7.x before 7.0.55, and 8.x before 8.0.9 does not properly handle attempts to continue reading data after an error has occurred, which allows remote attackers to conduct HTTP request smuggling attacks or cause a denial of service (resource consumption) by streaming data with malformed chunked transfer coding.

External References

- [CVE-2014-0227](#)

Classification

[OWASP 2010-A6](#) [OWASP 2013-A9](#) [PCI V2.0-6.1](#) [PCI V3.0-6.2](#) [PCI V3.1-6.2](#) [CAPEC-310](#)

12.1. /gratia-administration/images/

<http://gratia-main-osg.fnal.gov/gratia-administration/images/>

Identified Version

■ 6.0.24

Latest Version

■ 8.0.20

Vulnerability Database

■ Result is based on 4/22/2015 vulnerability database content.

Certainty



Request

```
GET /gratia-administration/images/ HTTP/1.1
Cache-Control: no-cache
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: gratia-main-osg.fnal.gov
Cookie: JSESSIONID=F1ED407F3CE0DDCFA012559C1794128E
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 404 Not Found
Date: Mon, 11 May 2015 19:58:47 GMT
Server: Apache-Coyote/1.1
Content-Length: 1042
Content-Type: text/html;charset=utf-8

<html><head><title>Apache Tomcat/6.0.24 - Error report</title><style><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-
size:14px;} BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color : #525D76;}--></style> </head><body>
<h1>HTTP Status 404 - /gratia-administration/images/</h1><hr size="1" noshade="noshade"><p><b>type</b></p><p><b>message</b></p><u>gratia-
administration/images/</u><p><b>description</b></p><u>The requested resource (/gratia-administration/images/) is not available.</u><p><hr size="1" noshade="noshade">
<h3>Apache Tomcat/6.0.24</h3></body></html>
```

13. Apache Web Server Identified

1 TOTAL
INFORMATION

Netsparker identified a web server (Apache) in the target web server's HTTP response.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

External References

- [Apache ServerTokens Directive](#)

13.1. /gratia-administration/

<http://gratia-main-osg.fnal.gov/gratia-administration/>

Certainty



Request

```
GET /gratia-administration/ HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: gratia-main-osg.fnal.gov
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Date: Mon, 11 May 2015 19:58:40 GMT
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"1038-1409755330000"
Content-Length: 1038
Content-Type: text/html
Last-Modified: Wed, 03 Sep 2014 14:42:10 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Frameset//EN" "http://www.w3.org/TR/html4/frameset.dtd">

<html>
<head>
<meta http-equiv="expires" content="-1">
<meta http-equiv="pragma" content="no-cache">
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
<meta http-equiv="Content-Language" content="en-GB">
<script language="javascript1.2" type="text/javascript">
<!--
// This page avoit to be shown under frames
if (top.frames.length==0) top.location=self.document.location;
//-->
</script>

<link href="stylesheet.css" type="text/css" rel="stylesheet">
<title>Gratia Accounting - Administration</title>
</head>
<frameset cols="21%,*">
<frame src="/dashboard.jsp" name="adminDashboard" id="adminDashboard" scrolling="auto" frameborder="1">
<frameset rows="37,*">
<frame src="admininfo.jsp" name="adminInfo" id="adminInfo" scrolling="no" frameborder="0">
<frame src="" name="adminContent" id="adminContent" scrolling="auto" frameborder="0">
</frameset>
</frameset>
</html>
```

14. [Possible] Internal Path Disclosure (*nix)

3 TOTAL
INFORMATION

Netsparker identified a possible internal path disclosure (*nix) in the document.

Impact

There is no direct impact; however, this information can help an attacker identify other vulnerabilities or help during the exploitation of other identified vulnerabilities.

Remedy

First, ensure this is not a false positive. Due to the nature of the issue, Netsparker could not confirm that this file path was actually the real file path of the target web server.

- Error messages should be disabled.
- Remove this kind of sensitive data from the output.

External References

- [OWASP - Full Path Disclosure](#)

Classification

[CWE-200](#) [CAPEC-118](#) [WASC-13](#)

14.1. /gratia-administration/adminlogin-howto.jsp

<http://gratia-main-osg.fnal.gov/gratia-administration/adminlogin-howto.jsp>

Identified Internal Path(s)

- /etc/gratia/collector/service-configuration.properties
- /etc/gratia/collector
- /usr/share/gratia/voms-server.sh
- /dev/null

Certainty



Request

```
GET /gratia-administration/adminlogin-howto.jsp HTTP/1.1
Cache-Control: no-cache
Referer: http://gratia-main-osg.fnal.gov/gratia-administration/dashboard.jsp
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: gratia-main-osg.fnal.gov
Cookie: JSESSIONID=F1ED407F3CE0DDCFA012559C1794128E
Accept-Encoding: gzip, deflate
```

Response

```
...
to have a certificate in your browser from
a trusted CA (Certificate Authority). This initiates the login process.
</p>

<p>The properties for the administration login can be found in the
<i>/etc/gratia/collector/service-configuration.properties</i> file set as
follows:
<pre>
# service.admin.DN.0=ALLOW ALL
# service.admin.FQAN.0=FQAN
# service.voms.connections=voms-servers
</pre>
</p>

<p>As you may have noticed above or if you have tried
...
ied by the top level group in the FQAN. In the 1st
example, it would be <i>cms</i>.
This is where the <i>service.voms.connections</i> property comes it to play. It identifies the file located in
<i>/etc/gratia/collector</i> that contains a list of the VOMS web service urls for each
VO.</p>
<p>The actual steps that the user will see are:</p>
<ol>
<li>A selection window will appear listing the VO (top level group) for
...
vo-client-edgmkgridmap-X-X.osg.noarch.rpm
</pre>

<p>The format for the <i>voms-servers</i> file is a
simple <i>VO</i>=<i>VOMS_URL</i> format.</p>

<p>The script that has been provided is:</p>
<pre>
/usr/share/gratia/voms-server.sh
</pre>

<p>This can be run manually or as a cron process. Running it as a cron process
is the recommended method since this insures any changes in VOMS service urls
is automatic.</p>

<p><font colo
...
ome VO's.
We hope to resolve this in the very near future.</font></p>

<p>In a non-VDT installation of Gratia services, you will have to set the <i>root</i> cron up
manually as:</p>
<pre>
42 1 * * * /usr/share/gratia/voms-server.sh >/dev/null 2>&1
</pre>

</body>
</html>
```

14.2. /gratia-administration/backlog-byprobes.html

<http://gratia-main-osg.fnal.gov/gratia-administration/backlog-byprobes.html>

Identified Internal Path(s)

■ /var/lib/gratia/collector-backlog-byprobes

Certainty



Request

```
GET /gratia-administration/backlog-byprobes.html HTTP/1.1
Cache-Control: no-cache
Referer: http://gratia-main-osg.fnal.gov/gratia-administration/backlog.html
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: gratia-main-osg.fnal.gov
Cookie: JSESSIONID=F1ED407F3CE0DDCFA012559C1794128E
Accept-Encoding: gzip, deflate
```


Response

```
...
_y_settings"/>Administrative security settings</td>
</tr>
<tr >
<td valign="top" class="property">service.voms.connections</td>
<td valign="top" class="explanation">File located in /var/lib/gratia-service/ containing the voms URL(s) for any
service.admin.FQAN attributes that are active.</td>
<td valign="top" class="example">Not set.<br/>Example: <code>voms-servers</code><br/>File can be updated
using <code>usr/share/gratia/<br/>voms-server.sh</code></td>
</tr>
<tr >
<td valign="top" class="property">service.admin.FQAN.<em>n</em></td>
<td valign="top" class="explanation">FQANs granting administrative pr
...
r >
<td valign="top" class="property">service.vdt.cert.file</td>
<td valign="top" class="explanation">Absolute path to vdt/does public cert file</td>
<td valign="top" class="example">/etc/grid-security/httpcert.pem</td>
</tr>
<tr >
<td valign="top" class="property">Service.vdt.key.file</td>
<td valign="top" class="explanation">Absolute path to vdt/does private key file</td>
<td valign="top" class="example">/etc/grid-security/httpkey.pem</td>
</tr>
<tr >
<td valign="top" class="property">service.autoregister.pem</td>
<td valign="top" class="explanation">Flag indicating whether or not external services (when runnin
...
<tr >
<td valign="top" class="property">service.ca.certificates</td>
<td valign="top" class="explanation">Location of trusted CA certificates.</td>
<td valign="top" class="example">/etc/grid-security/certificates/</td>
</tr>
<tr >
<td valign="top" class="property">service.ca.crls</td>
<td valign="top" class="explanation">Location of up-to-date CRLs for CAs.</td>
<td valign="top" class="example">/etc/grid-security/certificates/</td>
</tr>
<tr class="section" >
<td valign="top" colspan="3" class="section"><a name="reporting"/>Reporting</td>
</tr>
<tr >
<td valign="top" class="property">use.report.
```